

Subject Index to Volume 1

access control	1 (1982) 57
access controls	1 (1982) 231
ADP security	1 (1982) 210
analog scramblers	1 (1982) 275
annual security review	1 (1982) 139
application of cryptography	1 (1982) 113
architecture for security	1 (1982) 113
audit and evaluation	1 (1982) 164
audit trials	1 (1982) 123
auditability	1 (1982) 231
auditing	1 (1982) 57
auditing and security	1 (1982) 17
authentication	1 (1982) 146, 268
authenticators	1 (1982) 54
authorization	1 (1982) 99, 123
back-up techniques	1 (1982) 34
backup	1 (1982) 216
backup operations	1 (1982) 210
backup techniques	1 (1982) 99
banking and security	1 (1982) 226
Bureau of Standard	1 (1982) 255
cipher methodology	1 (1982) 177
classical cryptography	1 (1982) 177
communication delay	1 (1982) 275
communication protocols	1 (1982) 57
communication facilities	1 (1982) 34
communications security	1 (1982) 9, 226
computer abuse	1 (1982) 146
computer controls	1 (1982) 65
computer crime	1 (1982) 41, 99, 146
computer fraud	1 (1982) 9, 123, 139, 146
computer security	1 (1982) 17, 152, 210, 231
computer security bibliography	1 (1982) 164
computer vulnerability	1 (1982) 9
confidentiality	1 (1982) 65
contingency planning	1 (1982) 99, 123, 210, 216
control standards	1 (1982) 164
cooperative arrangements	1 (1982) 216
cost on control	1 (1982) 99
cryptanalysis	1 (1982) 57, 65, 72, 80, 164
cryptography	1 (1982) 27, 65, 164
cryptography bibliography	1 (1982) 57

- cryptology 1 (1982) 65, 177, 245, 249

- data accuracy 1 (1982) 123
- data encryption standard 1 (1982) 164
- data independence 1 (1982) 17
- data integrity 1 (1982) 9, 99
- data processing 1 (1982) 27
- data processing center failure 1 (1982) 34
- data security 1 (1982) 99, 113, 249, 255
- data security costs 1 (1982) 164
- DES 1 (1982) 261, 268
- disaster planning 1 (1982) 9, 34
- disaster recovery planning 1 (1982) 216
- distributed computer systems 1 (1982) 113

- economic 1 (1982) 245
- EDP auditing 1 (1982) 9, 17
- electronic funds transfer 1 (1982) 226
- electronic mail 1 (1982) 268
- emergency response 1 (1982) 210
- empty shells 1 (1982) 216
- encipherment 1 (1982) 65
- encoding 1 (1982) 65
- encryption 1 (1982) 65, 231, 268
- encryption techniques 1 (1982) 226
- environmental controls 1 (1982) 123
- executive guide 1 (1982) 233

- Federal Information Processing standards publication 1 (1982) 210
- fully configured service centers 1 (1982) 216

- hardware 1 (1982) 34
- hardware controls 1 (1982) 123
- hardware/software technology 1 (1982) 17
- hot site 1 (1982) 216
- human factors 1 (1982) 54
- hybrid cryptosystem 1 (1982) 268

- identification 1 (1982) 54, 99, 231
- identifiers 1 (1982) 54
- implementation 1 (1982) 261
- inspections 1 (1982) 201
- international computer law 1 (1982) 41

- knapsack problem 1 (1982) 72, 80

- local area networks 1 (1982) 268
- LSI chip 1 (1982) 261

- management control 1 (1982) 201
- management of computer systems 1 (1982) 17

- managing security 1 (1982) 9
- Merkle-Hellman trapdoor knapsack scheme 1 (1982) 72
- multiplicative inverse (Euclidean algorithm) 1 (1982) 72

- National Security Agency 1 (1982) 249
- NBS data encryption standard 1 (1982) 72, 177
- NBS data encryption system 1 (1982) 80
- network security 1 (1982) 164, 268
- non-deterministic polynomial problem (NP) 1 (1982) 72

- office automation 1 (1982) 113
- operating systems 1 (1982) 34

- passwords 1 (1982) 54, 123
- personal identification and access authorization 1 (1982) 164
- personnel policies 1 (1982) 139
- philosophical 1 (1982) 245
- physical security 1 (1982) 164
- physical security controls 1 (1982) 99
- privacy 1 (1982) 27, 65, 99, 268
- privacy and data 1 (1982) 17
- privacy regulations 1 (1982) 164
- privacy transformation 1 (1982) 65
- program controls 1 (1982) 123
- program library 1 (1982) 201
- protective measures 1 (1982) 57
- pseudo-code documentation 1 (1982) 201
- public key cryptography 1 (1982) 72, 255, 268
- public key distribution 1 (1982) 268
- public-key cryptosystem 1 (1982) 80

- recovery actions 1 (1982) 210
- recovery planning 1 (1982) 34
- residual intelligibility 1 (1982) 275
- risk analysis 1 (1982) 9, 99, 164
- risk analysis and assessment 1 (1982) 9
- risk management 1 (1982) 164
- Rivest-Shamir-Adleman scheme 1 (1982) 72

- secrecy 1 (1982) 65
- security 1 (1982) 27, 152
- security controls and safeguards 1 (1982) 164
- security policies 1 (1982) 139
- security staff training 1 (1982) 9
- security strategy 1 (1982) 17
- software piracy 1 (1982) 146
- software security 1 (1982) 9
- speech privacy 1 (1982) 275
- standards 1 (1982) 255
- structured programming 1 (1982) 201
- system integrity 1 (1982) 57
- systems development 1 (1982) 17
- systems integrity 1 (1982) 99, 123

technological	1 (1982) 245
terrorism	1 (1982) 41
top-down design	1 (1982) 201
training	1 (1982) 152
transborder data flow	1 (1982) 41
transmission robustness	1 (1982) 275
trapdoor problem	1 (1982) 72
two-dimensional scramblers	1 (1982) 275
use of librarians	1 (1982) 201
verification	1 (1982) 231
VLSI cryptosystem	1 (1982) 80
"walk-throughs"	1 (1982) 201
white-collar crime	1 (1982) 139

Author Index to Volume 1

- Akersten, S.I., see Blom, R. 1 (1982) 113
- Ball, L.D., Dentch, G., Emerson, M., Lewis, M., McWhorter, S. and Turgeon, F., Disaster Recovery Services 1 (1982) 216
- Banerjee, S.K., High Speed Implementation of DES 1 (1982) 261
- Block, H., see Lindén, C. 1 (1982) 226
- Blom, R., Brüer, J.O., Fak, V. and Akersten, S.I., On Security Measures in Distributed Computer Systems 1 (1982) 113
- BloomBecker, J., International Computer Crime: Where Terrorism and Transborder Data Flow Meet 1 (1982) 41
- Branstad, D.K. and S.K. Reed, Executive Guide to Computer Security 1 (1982) 233
- Branstad, D.K. and Smid, M.E., Integrity and Security Standards Based on Cryptography 1 (1982) 255
- Branstad, D.K., see Reed, S.K. 1 (1982) 231
- Brüer, J.O., see Blom, R. 1 (1982) 113
- Buck, R.C., The Public Cryptography Study Group 1 (1982) 249
- Carroll, J.M., The Control of Computer-Based Fraud 1 (1982) 123
- Courtney, Jr., R.H., A Systematic Approach to Data Security 1 (1982) 99
- Dentch, G., see Ball, L.D. 1 (1982) 216
- Emerson, M., see Ball, L.D. 1 (1982) 216
- Fak, V., see Blom, R. 1 (1982) 113
- Fordyce, S., Computer Security: A Current Assessment 1 (1982) 9
- Friedman, S., Contingency and Disaster Planning 1 (1982) 34
- Guillou, L.C. and Lorig, B., Cryptography and Teleinformatics 1 (1982) 27
- Henry, P.S., Fast Decryption Algorithm for the Knapsack Cipher 1 (1982) 80
- Highland, E.H. and Highland, H.J., A Guide to NBS Computer Security 1 (1982) 164
- Jayant, N.S., Analog Scramblers for Speech Privacy 1 (1982) 275
- Kahn, D., The Grand Lines of Cryptology's Development 1 (1982) 245
- Katzke, S.W., see Shaw, J.K. 1 (1982) 210
- Kurzban, S.A., A Selective, Briefly Annotated Bibliography of Works on Data Security and Privacy 1 (1982) 57
- Lewis, M., see Ball, L.D. 1 (1982) 216
- Lindén, C. and Block, H., Sealing Electronic Money in Sweden 1 (1982) 226
- Lorig, B., see Guillou, L.C. 1 (1982) 27

- McWhorter, S., see Ball, L.D. 1 (1982) 216
- Moulton, R., A Multidisciplinary Approach to the Investigation of Computer Abuse Incidents 1 (1982) 146
- Murray, W.H., Security Procedures for Program Libraries 1 (1982) 201
- Neugent, W., Teaching Computer Security: A Course Outline 1 (1982) 152
- Perry, W.E., Developing a Computer Security and Control Strategy 1 (1982) 17
- Porter, S.N., A Password Extension for Improved Human Factors 1 (1982) 54
- Reed, S.K. and Branstad, D.K., Reflections on Ten Years of Computer Security 1 (1982) 231
- Reed, S.K., see Branstad, D.K. 1 (1982) 233
- Schanning, B.P., Applying Public Key Distribution to Local Area Networks 1 (1982) 268
- Shaw, J.K. and Katzke, S.W., An Executive Guide to ADP Contingency Planning 1 (1982) 210
- Smid, M.E., see Branstad, D.K. 1 (1982) 255
- Turgeon, F., see Ball, L.D. 1 (1982) 216
- Willett, M., A Tutorial on Public Key Cryptography 1 (1982) 72
- Willett, M., Cryptography Old and New 1 (1982) 177
- Willett, M., Guest Editorial 1 (1982) 243
- Wood, C.C., Future Applications of Cryptography 1 (1982) 65
- Wood, C.C., Policies for Deterring Computer Abuse 1 (1982) 139